Aloha welcomes the opportunity to provide feedback to Ofcom's Consultation to potential measures, including the introduction of CLI Authentication in an attempt to reduce harm.

NOTE: This response to the consultation is based on our interpretation and understanding of the technological solution proposed which maybe subject to change.

Introduction

We are a strong believer in restoring the forever eroding confidence in our sector. Nuisance and Spam calls are becoming too associated to the landline. So much so that anecdotally most nuisance and spam calls originate from landlines and this could be behind the approx. 2/3 decrease in landline minutes over the past decade as highlighted in your consultation[1]. If we as a sector do not realistically find a solution, and fast, then ultimately there will not be much of a sector left for fixed line networks as less individuals will use them and the business sector will probably start losing suppliers as the market becomes more cut throat on smaller margins.

Therefore, we need to create a hostile environment for the spam caller taking the analogy of the Swiss Cheese model of cyber security, creating barriers here and there that make it more difficult to conduct illicit calls. As highlighted in the consultation, spam callers are omnichannel and agile in their methods. No single solution is going to stop them and therefore a package of solutions are required. We have seen this in the form of the DNO list[2] and the recent introduction of requirements from last year's CLI and Spam calls Consultation[3]. Although many of these changes only came into effect as of May 2023, we are already starting to see evidence that they may indeed be working as we've noticed an increase in enquires from non-UK organisations looking to send their UK CLI calls to the UK.

In our response to Ofcom's questions, we may have provided answers that could be relevant to other questions, but felt that specific question was the more appropriate location. Therefore, we have tried not to repeat ourselves wherever possible.

We'd like to point out given the material impact, over the coming years, we thought it prudent to emphasise the requirements on providers through the introduction of the Telecommunications Security Act 2021[4] and its subsequent secondary legislation (Electronic Communication (Security Measures) Regulations 2022[5]). This in a practical sense will result in the engineering bandwidth of CPs being mostly block booked until 2028 (and even so, some requirements maybe difficult to meet by then) who in some cases may need to completely redesign and redevelop their networks. Therefore, in the interest of mitigating harm to consumers, businesses and CPs we need to consider carefully what can be done to avoid road map fatigue as highlighted in the consultations third party report looking at CLI authentication

[1] https://www.ofcom.org.uk/__data/assets/pdf_file/0025/260656/CLI-Authentication-potential-approach-to-detect-and-block-spoof-numbers.pdf - Figure 2
[2] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/tackling-scam-calls-and-texts/do-not-originate
[3] https://www.ofcom.org.uk/__data/assets/pdf_file/0031/247486/statement-improving-accuracy-CLI-data.pdf - 4.135
[4] https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted
[5] https://www.legislation.gov.uk/uksi/2022/933/contents/made

based on experiences in North America[6]. The Ofcom consultation (as far as we can see) has made no mention of these statutory requirements and limits what can be done in the next 5 years from a technical solution as for integrity reasons network upgrades cannot be rushed in order to prevent a security compromise.

The switch-off of the PSTN in 2025 will enable Next Gen Voice to come into its own where many new technical features are possible. Although as with anything, just because something is technically possible, doesn't mean it is the best solution for the job. Like anything with new technology or solutions, there can be a fear of missing out when other countries are doing something new. Sometimes the best solution is to wait and see how teething problems have been overcome and then decide whether it's the right solution.

The United Kingdom has probably the most competitive, advanced, and developed telecommunication market of anywhere in the world. The truth is we have no idea how many CPs there are. Anecdotally many CPs are CPs without realising they are CPs. We can make an educated guess, but DCMS has recently highlighted how difficult it is to determine how many participants there are[7] and then there are subsets which are a fixed line CP, Mobile CP or Broadband CP who are then commonly split between a service provider and/or network provider (and maybe even an associated facility provider). Therefore, any solution must be realistically achievable in a way that is cost effective and possible given the number of market participants involved.

Although from a technical standpoint we like the idea of being able to understand the origin of a call in real time and verify CLI in real time (common number database), being implemented through the method suggested in the consultation, we must consider what our actual problems are and whether it will truly resolve them or at least materially reduce them. Although CLI Authentication would assist in preventing spoofing (with common number database), it wouldn't stop a spam call (if the technical make-up of the call is correct, for which many spam calls are).

Given the size of our sector (1000+ PECNs would need to work to a common date and that cannot be rushed), issues yet to be worked out (such as multi-homing) and the available engineering bandwidth for the foreseeable future including the cost of implementation and the cost of maintaining the solution we feel for now the CLI authentication idea is expensive, time consuming, potentially introduces security compromise risks, complicated to implement, not yet fully mature as a solution (based on the US experiences highlighted in the report) and ultimately is realistically probably 5-10 years away so will not achieve its aims any time soon. Furthermore, the solution would only assist in the subset of spam calls (potentially preventing spoofing) and would only practically assist law enforcement trace spam calls and would not actually technically prevent them (again only potentially stop spoofed calls should a common number database be implemented). For this reason, this is a significant amount of financial and technical resources focusing on a solution that ultimately may only limit a small portion of spam calls.

[6] https://www.ofcom.org.uk/__data/assets/pdf_file/0029/260678/shockey-report-issues-with-cli-authentication.pdf - 5.1

[7] https://www.legislation.gov.uk/ukia/2022/74/pdfs/ukia_20220074_en.pdf - 6.19

On the other side of this. We do have a wide range of ideas that we feel are worth a further discussion that we believe are quick, simple and efficient and could be implemented within several months:

- Quarterly Ofcom facilitated workshops with industry on nuisance/spam calls. This will allow CPs and the sector to be agile in identifying new trends.
- Enhance CP KYC on customers requiring CLI Authentication. This will help limit spoofing.
- CPs to investigate high volume low ASR/ACD Customers. This will help reduce spam calls and spoofing.
- Ofcom to reach out to industry trade groups of other sectors likely to be victims of spoofing to increase awareness of the DNO list. This will reduce spoofed calls.
- Enhance law enforcement SLAs and make CP abuse contact details better known. This will improve quicker traceability.
- CPs to keep supply chain details of a call for at least 6 months. This will improve traceability.
- Ofcom to consult the different uses of CLI Types. This will help provide clearer guidelines on CLI Types and how organisations can utilise CLI in next generation voice networks.

Question 3.1: Do you agree with our analysis of the ways in which number spoofing is used, and the extent and types of harm associated with its use? If you have any further evidence which demonstrates the extent and types of harm involved, please provide this.

Trust in the telephone networks is rapidly being eroded and that is not good for communication providers, the regulator, government or end users (consumers and business). Anecdotally, there is a lack of confidence in being able to trust an unsolicited, unexpected call making us second guess whether we really want to answer in fear of either being attempted to be sold something, upsold something or scammed (partially reinforced in 3.27).

In our view, we see number spoofing as a subset of scam/harm calls which in itself is a subset of nuisance calls. Although the difficulty with nuisance calls is it is subjective and technically the individual being called may have inadvertently consented to receiving such calls. As highlighted by our response (including that of another CP) to the CLI consultation in 2022[8] we asked Ofcom to review the different uses of CLI. We can find the current format of types going back almost 20 years[9] and may go back even further to pre-Ofcom. We still stand by what we said that the use of CLI may have evolved[10]. Given the general technological development, some businesses (even the smallest) may wish to be multi-homed for similar reasons the

[8] https://www.ofcom.org.uk/__data/assets/pdf_file/0031/247486/statement-improving-accuracy-CLI-data.pdf - 4.191

[9] https://www.ofcom.org.uk/__data/assets/pdf_file/0028/12988/cliguide.pdf

[10] https://www.ofcom.org.uk/__data/assets/pdf_file/0018/242325/Aloha-Telecoms.pdf - Response to Question 1.

largest wish to be as highlighted in your supporting documentation for this consultation. It also highlights that there is no accepted policy solution yet[11] and therefore Ofcom may need to conduct a sector wide consultation on how to better fulfil this requirement while keeping CLI safe from misuse. Furthermore, in response to point 3.12, we feel competitive rates and supplier redundancy are missing as a reason why the presentation number may be different. Tech savvy businesses want to be able to have more control over their caller ID. They may source numbers from one provider and use 2, 3 or more providers to route their calls through (e.g. provider 1 maybe more cost effective for landline calls, provider 2 maybe more cost effective for mobile and provider 3 is a backup). We are seeing this more often and from very small businesses.

In the voice market there are 2 sub-markets, Fixed Line and Mobile. Although the overall minutes over the past decade has remained fairly flat. The distribution has dramatically changed. Based on your sector minute usage research[12], over the past 10 years the amount of fixed line voice minutes has decreased by almost 66%. This means that fixed line is becoming a declining market, yet this is typically where new participants are entering. Furthermore, this is most likely the point of entry where nuisance/spam calls enter the telephony network. So, for a solution to have a higher chance of impact from source, it would need to be located at the fixed line network.

Over the past few years, we have seen Ofcom successfully start to reduce the amount of nuisance/scam calls such as dropped calls, quicker release on the PSTN, limiting spoofing in regard to well-known numbers (such as HRMC) through its DNO list initiative and through enhancing the requirements on how CLI should be handled for calls that originate from outside the UK. When combined, we call this creating a ‘Hostile Environment’ for spammers and scammers. Although it’s very early days, but we are of the firm opinion that the rules introduced in May (November CLI 2022 statement[13]) will noticeably reduce the amount of nuisance and potentially scam calls entering the United Kingdom from overseas. Why do we say this? As we have noticed a significant uptrend in international organisations looking for the ability to terminate their UK CLI calls into the UK where anecdotally it’s due to the rules introduced in May. Furthermore, the UK has now introduced surcharging, so this further introduces another layer of complication in calls originating overseas with a UK Network Number.

Although we agree spoof calls can help give a scam creditability, we are of the opinion (especially since the DNO list has become more popular) they make up a smaller amount of all the spam/nuisance calls. Furthermore, as highlighted by your research, scammers are omnichannel (3.28) and the phone can be just one channel that can be involved in the overall scam. It is important to be objective and proportionate. Building off the confidence point prior, the sector (especially the fixed line voice sector) is in a fight for survival. Minutes are down, competition is up and costs are up. Building on point 3.58 in your consultation it is known that

[11] https://www.ofcom.org.uk/__data/assets/pdf_file/0029/260678/shockey-report-issues-with-cli-authentication.pdf - 5.9

[12] https://www.ofcom.org.uk/__data/assets/pdf_file/0025/260656/CLI-Authentication-potential-approach-to-detect-and-block-spoof-numbers.pdf - Figure 2

[13] https://www.ofcom.org.uk/__data/assets/pdf_file/0025/260656/CLI-Authentication-potential-approach-to-detect-and-block-spoof-numbers.pdf - 4.135

random CLI from number ranges (typically where the numbers are not active but are live number ranges) can be spoofed causing time and effort for CPs in explaining that they themselves did not make the call. In response to the point raised in 3.64, it would be helpful as a sector if we had more up to date data as tactics do and frequently change in a forever cat and mouse game. It would be helpful if Ofcom over the coming months collaborates with other government bodies to determine how the recently introduced rules (specifically November CLI 2022 statement) are impacting the statistics, especially around spoofing and nuisance/spam calls as a whole. Therefore, we feel the recent enhancement around CLI and good practice for numbers will have a positive and hopefully material impact in reducing not just spoofed calls, but nuisance calls. However as highlighted in the previous consultation, our sector works on trust and it can result in just one CP being relaxed in their monitoring to ruin it for everyone else.

Question 4.1: Do you agree with our assessment that while Ofcom rules and industry measures are likely to help to reduce scam calls, more needs to be done to tackle number spoofing? Provide reasons for your answer and include any suggested measures that could have a material impact on reducing the incidence of scam calls involving number spoofing.

We feel it is paramount and material to highlight when working out implementing such a significant change to network infrastructure is the volume of CPs who operate within the UK market (defined by the Act). As highlighted recently by DCMS in their Telecom Security Regulation framework impact assessment, it's difficult to estimate how many participants there are in the market[14]. DCMS commissioned research into the size of the market between October 2021 and February 2022 and determined there were about 4,000 CPs based on SIC codes[15]. Although SIC code is no guarantee. Ofcom's public data can put this in the higher[16] and low thousands[17]. Realistically, it's probably in between (perhaps 3,000-5,000 CPs which reinforces DCMS's findings). A good portion of these would be a PECN (defined by Section 32[18] and 151[19] of the Communications Act 2003) in that they control the routing of outbound calls and source ranges directly from Ofcom or acquire sub allocations from other CPs (which can be range holders or reselling themselves). Anecdotally we put this in the region of around 1,000 PECNS. They will then typically route their calls out via multiple CPs for cost effectiveness and resilience.

We are very supportive of the DNO list and believe it is a rapid solution for inbound only numbers, we do agree in regards 4.16 in which you highlight its limitation for numbers used to also make calls. Therefore, it's important to set expectations of what is and what isn't possible (especially to the non-Telco industry). Realistically we will not be able to all stop

[14] https://www.legislation.gov.uk/ukia/2022/74/pdfs/ukia_20220074_en.pdf - 6.19

[15] https://www.gov.uk/government/publications/telecommunications-providers-survey-october-2021-to-february-2022/telecommunications-providers-survey-october-2021-to-february-2022-research-notes - methodology

[16] https://www.ofcom.org.uk/__data/assets/excel_doc/0029/227783/RID.xlsx

[17] https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/problems/adr-schemes

[18] https://www.legislation.gov.uk/ukpga/2003/21/section/32

[19] https://www.legislation.gov.uk/ukpga/2003/21/section/151

scams, spoofing, nuisance calls, but what we can do is reduce, share intelligence and possibly apply a risk based, intelligence led approach. CPs in collaboration with the regulator and industry can create a hostile environment for scammers and taking the analogy of the Swiss Cheese model of cyber security, create barriers here and there that make it more difficult to conduct illicit calls. Furthermore, CPs will typically have data readily available to them which can be key indicators of spam, nuisance and possibly upon investigation spoofing as well. This is discussed further below.

In terms of a phone call, call establishment is typically the most system resource intense part of a phone call. This is due to various checks being conducted (potentially up to 250,000+ per phone call) such as to determine where to route the call, whether the network number and presentation number are allocated by Ofcom (approx. 125,000 ranges) and this is fairly resource intense. Building off your point further in 4.34(b), 2 of the main indicators that to determine overall call efficiency is the Answer Seizure Ratio (ASR) and the Average Call Duration (ACD). The first is of all the total call attempts, how many answered and the second is of all the calls that answered what was the mean time of them. Typically, low ASR and ACD are primary indictors that an account may being used for illicit purposes. Obviously, businesses of all sizes maybe having a bad day (perhaps no one is answering that day), but continual frequent days where there are high volume attempts would suggest something needs to be investigated further. There could be a bona-fide reasons for low ASR and/or ACD where current customers of the business have agreed to receive marketing calls (or could be canvas members of a political party who have agreed to be called). In the example above, both could have similar stats, although in reality this could prompt a CP to make a note about the customer for next time or to put a note when onboarding. A CP realistically though will not want a customer to have a low ACD/ASR as its very resource intense and the issues highlighted in 4.43 apply equally to CP checks (i.e. the more checks (numbers added to be checked), the more inefficient it becomes). A call going through 250,000 data point checks can easily have 0.1 second added to its call establishment time. Although this may not sound long, if there are several PECNs upstream all conducting the same checks (which the rules technically require each and every CP to do) then if there are 5 CPs involved (which can be plausible based on US experiences as highlighted in a footnote of your consultation[20]) in the call chain, 0.5 seconds delay could easily be added to each call which can result in overall slower voice networks.

Combining the points raised so far in our response, it is most likely nuisance, spam and spoofing calls originate from customers of fixed line CPs. It's also highly likely that of those fixed line CPs, the majority of the market CP participants are small (micro) businesses. Given the ease that some can become a PECN (£5/mth virtual machine) it's highly likely that any solution developed needs to realistically be within the technical and economically capability of that CP.

Since your consultation in 2019[21], the world is very different. We have come through a pandemic that saw CPs (especially smaller CPs) become extremely agile to assist their

[20] https://www.ofcom.org.uk/__data/assets/pdf_file/0025/260656/CLI-Authentication-potential-approach-to-detect-and-block-spoof-numbers.pdf - footnote 159

[21] https://www.ofcom.org.uk/__data/assets/pdf_file/0022/144265/first-consultation-promoting-trust-in-telephone-numbers.pdf

customer base adopt to a work from home environment. Furthermore, we are currently in a situation where the economic outlook is uncertain, interest rates are raising, debt is become for more expensive to service and keeping all the servers that run Next Generation Voice telecom networks are getting more expensive to run due to electricity costs. This is not to mention margins are getting smaller and customers are expecting more for less, so resources have to be used in a highly efficient and proportionate way. Furthermore, the UK has probably the most advance, largest and diverse telecommunication eco system in the world so any major network changes would need to be choreographed years in advance. Building off this, we also have the recently introduced Telecommunication Security Act and its accompanying Regulation with a staggered implementation time until 2028[22]. This means that in some cases CPs may need to rebuild entire parts of their infrastructure to meet the key milestones set out in the code of practice up to 2028.

It's important that any technical solution does not add significant power consumption to a provider networks. As highlighted above, if all CPs in the chain are conducting checks, it could increase call establishment delays, but also increase the sectors power footprint materially (not to mention potential increases in emissions). For example, should the proposed consultations solution be implemented, based on today's technology, it would add about 250 watts to our own network footprint usage. Although this may not sound much (considering a kettle uses 2000-3000 watts for a minute or 2 while boiling water), this is 24/7/365 operation and its likely a larger CP would be considerably higher (in the multiples of Kilowatts). If all CPs have to implement (working on 250 watts per CP; some CPs will be much higher, others maybe a little less) we calculate that this will increase the sectors energy footprint by 2-3GwH per year (on the assumption there are 1,000 voice PECNs)[23] and based on where electricity prices (£0.50 per Kwh; although varies greatly) could easily cost the sector over £1,000,000 a year in running costs that would be put more on the smaller CP to bear the brunt of the overall costs (as that is where most PECNs by volume are in the market based on turnover). Furthermore, such a cost could negatively impact the costs of consumers and small business as these kind of costs in a declining market have an impact on FTR and possibly MTR cost calculation.

We feel that given the issue spam and nuisance calls are becoming, we feel that an agile approach is required to an ever-changing landscape. We do have some ideas we think could help the knowledge sharing and agility of the sector along with other requirements that could help limit nuisance and spam calls including the spoofing of numbers. These are some initial ideas that we feel warrant further discussion and consideration:

- **Quarterly Ofcom facilitated workshops with industry on nuisance/spam calls.** We would like to see Ofcom run (or delegate it to an organisation such as the OTA) a quarterly workshop/call with the sector to discuss trends CPs are noticing to highlight new tactics and potential solutions to limiting nuisance, spam and spoofed calls.

[22] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1120531/E02781980_Telecommunications_Security_CoP_Accessible.pdf

[23] ((250 watts (per cp) x 8760 hours (per annum)) / 1000 (convert to KwH)) x 1000 (approx. PECNs) = 2,190,000 KwH

- **Enhance CP KYC on customers requiring CLI Authentication**
  Require CPs to conduct better KYC on anyone (including commercial contract CPs; not to be confused with interconnect agreements under SMP access) to take the ID of the directors if the business is small or less (Companies Act definition[24]) of anyone who requests CLI flexibility either at a Network Number level (typically other CPs) or presentation number level (e.g. Type 5 CLI presentation)

- **CPs to investigate high volume low ASR/ACD Customers**
  As highlighted above, require CPs to actively monitor ACD/ASR stats and investigate low levers and put a few common appearing CLIs into a search engine to see what comes up (e.g. high complaints about a number or suspected spoofing). If a CP has concerns, then it should request evidence it has the authority to show that CLI(s) (e.g. Letter or Authority), is redirection CLI (i.e. the CLI is coming in and being redirected back out which typically should be confirmed via a paper trail through audit) or the individuals who are being called have explicitly agreed to be contacted (e.g. requirements set out under the Data Protection Act / PECR). We feel all CPs at all levels should be involved in this level of checking ASR/ACD stats and further investigating irregularities. This idea is similar to how in the Financial Services Sector each party involved in the transaction (in our example the call) has shared responsibility in preventing terrorism funding.

- **Ofcom to reach out to industry trade groups of other sectors likely to be victims of spoofing to increase awareness of the DNO list**
  There is only so much CPs can realistically and reasonably be required to do. Ofcom has a fantastic, track record proven tool that can quickly stop number spoofing (in many, but not all cases). It needs to make better use of this and go out to other sectors (which are potentially targets for spams, misuse and impersonation) such as (if not already contacted) the energy sector, the home delivery sector to name but a few. This could be streamlined by reaching out to industry bodies which represent these organisations who can pass on information about the DNO list and how to get numbers added to it.

- **Enhance Law Enforcement SLAs and make CP abuse contact details better known**
  As suggested in our response last year to the Spam consultation[25], we believe that CPs should have an SLA for replying to a law enforcement request and should put details on their website where to send law enforcement requests.

- **CPs to keep supply chain details of a call for at least 6 months**
  To allow reasonable time for law enforcement and government bodies to be made aware of a scam and assist in their enquiries, data should be available for a reasonable period of time (e.g. 6 months) so they can say a call was handed over from X CP or sent to Y CP. Although this may need further investigation to determine whether this is compatible with interconnect agreements. Although if you know the origination number, the range holder details are public.

[24] https://www.legislation.gov.uk/ukpga/2006/46/part/15/chapter/1/crossheading/companies-subject-to-the-small-companies-regime

[25] https://www.ofcom.org.uk/__data/assets/pdf_file/0018/242361/Aloha-Telecoms.pdf - Response to Question 5

- **Ofcom to consult the different uses of CLI Types**
  This will help provide clearer guidelines on CLI Types and how organisations can utilise CLI in next generation voice networks. The current rules can be found going back almost 20 years and ultimately may even predate Ofcom. It's reasonable to think CLI uses may have changed over that time period.

Question 5.1: Is the approach to CLI authentication we have outlined feasible and workable?

Our feelings are mixed in relation to the initial approach for CLI Authentication in the UK. Technically we believe the solution itself is workable and would provide benefits to be able to trace call origins. However, practically we cannot see the solution working in the United Kingdom without a significant structure change to the whole PECN market given the volume of participants (or at least a better idea of how many participants there are). The reason for this is because we have a very diverse and large PECN market size and the idea that 1,000+ CPs having to implement this for it to work we don't see as feasible. As highlighted in the report prepared on behalf of Ofcom[26], for this to be effective, all PECNs would potentially have to implement and if our understanding is correct could not rely on CPs upstream with greater technological expertise to implement. This is because smaller CPs (who are not range holders) in our experience source numbers from multiple suppliers and route their calls out via multiple CPs which means they would need to be able to have the number assigned to them in any common numbering database and would need to sign a call themselves. Although this may not be impossible, it would need greater discussions and consideration before a formal decision is made to see if any viable solutions could exist for smaller PECNs. Furthermore, it may push more PECNs to become range holders and could cause further constraint on the supply of number ranges or for Ofcom to consider allocating ranges in blocks of 100 (which they do for a small number of areas) than the typical 1,000 or 10,000 blocks.

In addition, it needs to be continually brought to the forefront of one's mindset that the reason for this is primarily to prevent number spoofing. However without additional implementation (through a common number database) the solution will not actually stop or technically prevent number spoofing. The consultation report[27] conducted on behalf of Ofcom highlights some of the major milestones which have been seen in the North American implementation and why we feel they may cause material issues in the implementation within the UK:

- **Multi-homing Issues (smaller and larger businesses)**
  There are issues yet to be worked around multi homing[28] which businesses of all sizes are requesting more commonly (especially since Covid) and are becoming more commercially savvy (i.e. want to split their routing options). Changes which could impact this could cause significant issues in businesses increasing their resilience and

[26] https://www.ofcom.org.uk/__data/assets/pdf_file/0029/260678/shockey-report-issues-with-cli-authentication.pdf - page 2
[27] https://www.ofcom.org.uk/__data/assets/pdf_file/0029/260678/shockey-report-issues-with-cli-authentication.pdf - Chapter 5
[28] https://www.ofcom.org.uk/__data/assets/pdf_file/0029/260678/shockey-report-issues-with-cli-authentication.pdf - 5.9

being multi-homed. The report did discuss solutions, but this needs further consideration.

- **Technical bandwidth for major network changes is limited for the next 4-5 years**
  The Ofcom consultation makes no mention of the new Telecom Security Act and its secondary legislation (Electronic Communication (Security Measures) Regulation 2022) obligations that may require CPs to potentially redesign, redevelop and reimplement there entire infrastructure over the coming years (up until 2028) where deadlines are tight. The idea of adding significant call filtering technology will certainly increase the likelihood of roadmap burn out as highlighted by the report prepared on behalf of Ofcom[29].

- **Mass update of interconnects needed**
  As highlighted in the report, many CPs are still using UDP[30]. Therefore, migrating to TCP (which the report suggests is highlighted to prevent dropped calls due to packet fragmentation[31]) would require every CP (who is not using TCP) to re-interconnect with each other which would be a logistical nightmare given the scale of PECNs, the amount of telephony switches and how many interconnects each PECN could have. Although counter to this, based on our understanding the new Telecom Security Regulations does currently have a requirement on the encryption of the signal by 2028[32,33]. Current technical solutions for encryption do use TCP, however (from our understanding) currently there is no industry agreed encryption protocol in the United Kingdom and given the complexities of everyone re-interconnecting and the workload put on network teams, this will require Ofcom, NCSC and DSIT/DCMS collaborative input and guidance on how they foresee this exactly working. 2028 is 4-5 years away and the amount of time required could easily exceed that and either see/require that requirement being removed completely or extended until the mid 2030's (especially since there's not even an industry standard yet).

The TSA/TSR requirements put a requirement on the supply chain[34], so any solution (including that by the CLI Authentication Administrator) will have to meet strict technical security standards which could enhance the cost of any solution through compliance. Building off this, and we appreciate there is further discussion needed around this, but as partially highlighted around call setup delays. If each and every call is going to require a number to be checked, where will this information be stored? If as a CP we need to make an API call (for every call) to a common numbering database, then this introduces extra delays (as its not cached internally inside our network for faster lookups) and creates a risk by the way of us having to rely on the uptime and low latency of the CLI Authentication Administrator's infrastructure.

[29] https://www.ofcom.org.uk/__data/assets/pdf_file/0029/260678/shockey-report-issues-with-cli-authentication.pdf - 5.1

[30] https://www.ofcom.org.uk/__data/assets/pdf_file/0029/260678/shockey-report-issues-with-cli-authentication.pdf - 5.3

[31] https://www.ofcom.org.uk/__data/assets/pdf_file/0029/260678/shockey-report-issues-with-cli-authentication.pdf - 5.3

[32] https://www.legislation.gov.uk/uksi/2022/933/regulation/4/made - Regulation 4, Clause 5

[33] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1120531/E02781980_Telecommunications_Security_CoP_Accessible.pdf - Page 104 - Signalling Plane 4

[34] https://www.legislation.gov.uk/uksi/2022/933/regulation/7/made - Regulation 7

On the flip side of this, if we were to cache and there being potentially 1000+ PECNs who would all need to have regular access to this list, would we want 1000+ CPs having access to every allocated/in use number in the United Kingdom? I'd like to think more of our sector, but should the list get into the wrong hands then it would be a spam callers haven. This needs further consideration and thought.

Building off the above, CPs rushing to implement all of these changes in itself could introduce widespread sector integrity issues which the act/regulation aims to avoid. So it's important roadmaps are reasonable and realistic. It's important any technological changes to the sector are well thought out, discussed and are regularly reviewed to adapt to any unforeseen problems that had not been considered. This is partially highlighted in the report prepared on behalf of Ofcom[35].

Overall, we are supportive of the solution methodology (with a common numbering database), but we have to be realistic around time frames, any technical challenges and whether it's really going to make a material impact on its own to the greater issue.

Ultimately, if we are as a sector are to work towards this, then it maybe prudent to setup a working group that any CP/Industry trade body can join to work out all the challenges and agree solutions forward.

Question 5.2: To what extent could adopting this approach to CLI authentication have a material impact on reducing scams and other unwanted calls? If you consider an alternative approach would be better, please outline this and your reasons why.

If (and that is a big if) all the challenges are overcome as highlighted in our response to 5.2 (and other questions) AND the UK introduces a common numbering database, then actually we feel this would work extremely well in preventing spoofed calls (not fool proof, but certainly would prevent a good portion of calls). However, we're sceptical whether it would have a material impact on reducing scam calls and other unwanted calls as scam calls are not necessarily found out until some time has passed (although it would enhance traceability) and unwanted calls is "subjective" in the sense that a customer may have legally opted in or consented to being called. Ultimately though it is down to the correct authority identifying the scam and following up. A CP will not know a caller is a Scam without there being complaints or some due diligence work (which we've highlighted as an area where CPs can go further such as looking at ASR/ACD stats).

Furthermore, we feel a subjective costs vs benefits should be conducted between the current DNO list we have and proposed CLI authentication (with common numbering database). Organisations who are targets of spoofing (along with other stakeholders involved) all need to a play a part and if they are victims of this, then they need to consider whether they forego the ability to make outbound calls with their number so the number can be added to the DNO list. Furthermore, where spoofing is used to build confidence in the victim, then perhaps

[35] https://www.ofcom.org.uk/__data/assets/pdf_file/0029/260678/shockey-report-issues-with-cli-authentication.pdf - Chapter 9

where numbers are given on documents, a short text saying “We do not make calls from this number” could be added. This could prompt a victim to consider who’s calling if they are asked to check the number to verify it is them (e.g., on the back of their bank card).

Question 5.3: Are there additional measures that could be adopted to further strengthen the suggested approach and/or minimise the identified exemptions?

If the UK were to introduce CLI authentication, then we’re of the opinion it needs to be done properly and as such the common numbering database must be implemented from day one. Otherwise objectively, we see little benefit in the whole solution.

Question 6.1: Do you agree with the approach outlined for the monitoring and enforcement of the rules with regard to CLI authentication? Are there any alternative approaches that we should consider?

In general we do agree, although should Ofcom find a CP is continually not correctly authenticating calls (not through intentional means, but unintentional due to financial or technical ability means) would Ofcom really seek to revoke their ability to call (e.g revoke certificates)? Although Ofcom may have the legal right and could seek other enforcement regimes (such as through a fine), revoking a certificate should be the absolute final last case scenario. Maybe a solution that would need further discussion to find a means, perhaps through a working group, is to find a solution where only more technically integrated CPs need implement the solution. At this stage we cannot think of one though.

Question 6.2: Do you agree that CLI authentication could make call tracing easier and yield benefits in terms of detecting scammers and nuisance callers?

Without a common numbering database, in our view this is one of the only benefits of CLI authentication (in that you know which PECN CP a call originated from), although if the customer facing CP has multiple PECS in terms of supply chain on the PECN, then it could still mean there could be delays in getting the end customer data due to finding which ultimate CP who owns the customer which is the issue we have today.

Furthermore, we’re concerned to hear (unless we’ve misunderstood something) that some CPs only keep their call records for a few days (6.28). A billing issue between CPs may not come to light until several months after the call and may need to be reconciled to identify a billing fault. Likewise, CPs should be keeping call records to produce bills to bill their customers. There may also be requirements on some CPs to retain specifc data for upto 12 months[36]. Likewise, though if some CPs are only keeping their data for short periods of time, then this would likely be the same for any Passport identify information of where a call originates from. This is not to say a call record may contain non billable detailed technical information related to the call (such as codec) which may only have a short requirement (in the case of technical

[36] https://www.legislation.gov.uk/ukpga/2016/25 - Investigatory Powers Act 2016 – Part 4

troubleshooting) before being deleted. Requiring CPs to keep call data related to supply chain for at least 6 months could assist in traceability.

Question 7.1: What are your views on the timescales for the potential implementation of CLI authentication, including the interdependencies with legacy network retirement?

We believe the earliest realistic time period (for reasons stated prior around current sector roadmaps and issues that need to be worked out) is probably late 2020's, early 2030's. With CPs having to work to close time scales in respect of TSA/TSR obligations and the PSTN shut down, the roadmap is fairly full for any significant technical developments until 2028 (not to suggest there may not be extensions and unforeseeable issues as highlighted around encryption, but this equally may provide an opportunity for CPs to convert to TCP on their interconnects as encryption is typically TCP). Therefore, for this reason, given the PSTN 2025 switch off we don't see legacy networks having an issue.

Question 7.2: Do you agree with our assessment of the administrative steps required to implement CLI authentication and how these should be achieved?

We agree that CPs are best placed to decide the best approach. However, should there be further discussion around implementing CLI authentication, we would like to see an Ofcom ran and led working group that CPs and industry bodies can join and discuss with other CPs/industry bodies. Our logic behind this is that given the critical importance of call/CLI filtering and the integrity issues it could introduce if there are unforeseen issues, it's important that every CP has the option to be part of the conversation through a transparent, open technical discussion about problems including their ideas for solutions (similar to how porting solutions and problems are resolved). Furthermore, CPs large and small are all running potentially different network topologies so it's important smaller networks (those who will outnumber the larger providers in terms of technical solutions/implementations) will need to make sure that solutions of implementation are agreed and realistic within the financial and technical means of that CP. Although Ofcom typically stays technology/solution neutral, smaller CPs on this topic may indeed be looking to Ofcom for guidance.

Question 7.3: Should a common numbering database be implemented to support the CLI authentication approach? Please provide any comments on the steps needed to implement a common numbering database, including on the feasibility of the industry leading on (a) the specification; and (b) the implementation?

We believe that a common numbering database should be implemented from day one if CLI authentication is implemented as that is true CLI authentication in the plain English sense (i.e. a CLI is checked for its authenticity). Otherwise, its CLI in name only (as CLI is not authenticated) and there is very little benefit except assisting government bodies on where a call originated from which then it potentially creates a Moral Hazard where CPs (especially smaller CPs) are bearing the cost for other government department benefits.

As highlighted above a solution needs to be determined how CPs can cache to reduce potential call establishment delay (especially when multiple CPs are involved in the call chain potentially all doing the same check), but in a way that a list of all the active numbers in the UK does not potentially get into the wrong hands due to a malicious or accidental leak (more probable). Furthermore, there needs to be the ability for CPs who are provided sub allocations (including those resold multiple times through the supply chain) to have numbers assigned to them (likewise required in porting).

Question 8.1: Do you agree with the proposed framework for impact assessment and the potential categories of costs and benefits? Please identify any other factors that we should take into account in our assessment.

We agree with the 3 proposed objectives in your impact assessment framework, although we feel there needs to be another 2 objectives that objectively look at the cost and implementation time. If a solution is going to take a very long time to implement and cost a significant amount of money to implement then harm will continue while the solution is implemented, but ultimately will also be factored into higher bills for the customer (directly) and taxpayer (indirectly).

In respect to your analysis of the 3 objectives considering CLI authentication we agree mostly with your analysis although we do disagree in a few areas:

- Objective 1 we'd like to highlight that we'd only seldomly agree with your objective 1 points if a common numbering database was mandated as otherwise we'd see very little point of benefit in introducing it in the attempt to reduce harm.
- Objective 2 – We disagree with the benefits highlighted for business. If anything it could cause issues around multihoming as highlighted in the consultant's report. Therefore, reducing flexibility currently enjoyed by businesses. Furthermore, although we agree (if with a common numbering database) could possibly restore some confidence in the telephony market, it won't stop all nuisance calls or some scam calls as technically everything could be correct, but it could assist in tracing them quicker.
- Objective 3 – We'd like to add that there would be initial and ongoing security costs (including penetration testing) to confirm the solution is secure and meets the requirements under Regulation 7 (including others) of the Electronic Communications (Security Measures) Regulation 2022[37].

[37] https://www.legislation.gov.uk/uksi/2022/933/regulation/7/made - Regulation 7